The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
11/10/2009

SUBJECT:
Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (MS09-067)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Office Excel. These vulnerabilities can be exploited by opening a specially crafted Excel document. The document may be received as an email attachment, or by visiting a web site where the document is posted. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Microsoft Office XP
Microsoft Office 2003
Microsoft Office 2007
Microsoft Office 2004 for Mac
Microsoft Office 2008 for Mac
Open XML File Format Converter for Mac
Microsoft Office Excel Viewer
Microsoft Office Compatibility Pack

RISK:

Government:

Large and medium government entities: **High**
Small government entities: **High**

Businesses:

Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
Eight vulnerabilities have been identified in Microsoft Office Excel that could allow an attacker to take complete control of an affected system. The vulnerabilities can be triggered by opening a specially crafted Excel document (.XLS). These vulnerabilities can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted Excel document as an email attachment. In the Web based scenario, a user would have to be convinced to visit a website and then open the specially crafted Excel document that is hosted on the page. When the user opens the Excel document the attacker's supplied code runs.

Please note that Microsoft Office XP or higher will, by default, prompt the user to Open, Save, or Cancel when accessing Office files in a Web or e-mail based scenario.

Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS09-067.mspx

Security Focus:
http://www.securityfocus.com/bid/36943
http://www.securityfocus.com/bid/36944
http://www.securityfocus.com/bid/36945
http://www.securityfocus.com/bid/36946
http://www.securityfocus.com/bid/36908
http://www.securityfocus.com/bid/36909
http://www.securityfocus.com/bid/36911
http://www.securityfocus.com/bid/36912

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3127
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3128
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3129
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3130
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3131
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3132
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3133
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3134